UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Supplemental (S) Questions and Answers Regarding Increased Controls (IC) and Implementation for Licensees That Possess Radioactive Material Quantities of Concern

Table of Contents

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S1. Who should we contact to handle issues that arise regarding the Increased Controls, or related issues? Also, where should responses to issued Orders be sent?

As Q&A #11 indicates, there is NRC or Agreement State contact information provided in the letter transmitting the increased controls requirements.

For NRC licensees who are seeking resolution of any issues or have questions about compliance with the requirements in the Order, you may call Increased Controls Support at (301) 415-7197, or e-mail questions to ICSupport@nrc.gov. Correspondence can also be sent via fax at 301-415-5369, and should be addressed to the attention of Ernesto Quinones, Mail Stop T8F3.

NRC licensee responses to the Order are required to be submitted to the Director, Office of Nuclear Material Safety and Safeguards. The following mailing addresses should be used:

For normal postal delivery, mail to:
Director, Office of Nuclear Material Safety and Safeguards
U.S. NRC
Washington, DC 20555-0001
ATTN: Ernesto Quinones, Mail Stop: T8F3

For delivery services requiring a street address, mail to:
Director, Office of Nuclear Materials Safety and Safeguards
U.S. NRC
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738
ATTN: Ernesto Quinones, Mail Stop: T8F3

Note that licensees requesting a hearing should follow instructions in Section IV of the Order.

S2. Do the Increased Control (IC) requirements apply to unsealed radioactive material? For example, do the requirements apply to materials possessed by a nuclear laundry or radioactive waste processor?

There is no distinction between unsealed and sealed radioactive material when implementing these ICs. A licensee must implement the ICs if they possess radioactive material in quantities that meet or exceed the Table 1 values (including aggregation). However, a licensee may request relief from its appropriate regulatory agency, if the licensee believes that compliance with the ICs is unnecessary because the radioactive material it possesses is well dispersed and is not easily aggregated into quantities that meet or exceed the Table 1 values. If relief is requested, a licensee needs to demonstrate that all radioactive materials resulting from waste processing do not meet or exceed the Table 1 thresholds. Therefore, relief from implementation of the ICs shall be evaluated on a case-by-case basis.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S3. How would fixed gauge licensees determine if the sources in their devices are considered co-located?

The sources or devices containing the sources are considered co-located, if breaching a common physical security barrier to allow access to the sources or devices. For example, multiple fixed gauges in a facility where all gauges are accessible after passing through a perimeter security check point, or by breaching a perimeter fence, would be considered co-located. However, if additional physical security barriers are present within the facility that would prevent access to quantities of radioactive material that exceed a Table 1 quantity, then the sources or devices are not considered aggregated or co-located and implementation of the Increased Controls (ICs) is not required. Examples of physical barriers for fixed gauges may include locked enclosures such as rooms, cages, and metal enclosures that completely encase the gauge and are permanently attached to some other immovable object (large pipes, tanks, beams, solid floor/ceiling, etc.). Examples of non-permanent physical security barriers include robust cables or chains with locks, tamper proof mounting bolts (such as one way threading or welded in place), or using locks to prevent removal or disassembly of gauge mounting hardware (e.g., that pass through mounting bolts or through the housing and mounting plates). Currently, Q&A #124, provides guidance that suggests a heavy-duty twisted steel wire cable which can be used to secure portable and mobile devices. As with any system, a barrier is only as strong as its weakest component. Therefore, in order for a licensee to consider a physical barrier to be effective (or to take credit for the barrier), the licensee must ensure the barrier cannot be bypassed or easily defeated using commonly available tools. Also, a licensee has to be aware that at anytime, a physical barrier that has been installed to isolate remaining co-located gauges from a gauge is breached (e.g., during source exchange) therefore totaling the quantity that would meet or exceed the Table 1 quantities, would then require the licensee to implement the ICs.

Unique cases that are not addressed by the ICs or the guidance will be evaluated on a case-by-case basis if relief is requested.

S4. If a research reactor licensee possesses a Research and Test Reactor (RTR) security plan and/or is implementing the security Confirmatory Action Letter (CAL) for radioactive material that is at levels that are equal to or greater than the Table 1 thresholds in the RTR controlled access and protected area (under Part 50 jurisdiction), can an exemption from the Increased Controls (ICs) be granted to this licensee?

The reactor bay falls within the scope of the NRC-approved physical security plan, however the plan may not meet all the requirements for ICs. Also, radioactive materials that are at levels that are equal to or greater than the Table 1 thresholds of concern may be used outside the RTR controlled access and protected areas at certain times.

Although the security plan and CAL response may be adequate for implementing some or all of the ICs, it is the licensee's responsibility to ensure that all of the ICs are satisfied at all times. Therefore, the Order shall remain in effect and an exemption to the ICs shall not be granted.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S5. Can a partial exemption to IC 2. be granted to licensees at extreme remote locations (off-shore and in extreme wilderness locations), where access is limited and communication is difficult, on a case-by-case basis?

Remoteness may allow an intruder to successfully gain undetected and unauthorized access more readily than in more populated environments. The time for discovery may be increased as well, which results in the success to any intruder who has the intent to steal or sabotage the material. Success by the intruder means failure for the licensee relative to IC 2. b. Therefore, the licensee shall meet the requirements of all the Increased Controls (ICs). If the licensee believes that it cannot meet portions of the IC requirements, for example IC 2. b. because of remoteness and distance from a Local Law Enforcement Agency, the licensee shall provide justification for relief to those portions of the IC and provide compensatory measures to meet the requirements of those particular sections of the ICs. The requests for relief will be evaluated on a case-by-case basis.

S6. Would disengaging a standard key from a vehicle's ignition be considered a means to "disable" a vehicle when a vehicle or trailer is not under direct control and constant surveillance by the licensee as required in IC 4. c.?

Removing a standard key from a vehicle's ignition cannot be considered sufficient for disabling a vehicle's engine because there are means to start a vehicle without a key, such as using a duplicated key or hot-wiring techniques. A licensee needs to either keep the vehicle under direct control and constant surveillance or disable it using techniques similar or equivalent to those recommended in the existing guidance (i.e., guidance provided in Q&A #125).

There are currently many advances in ignition and key technology that provide for additional barriers that would cause delay in accessing radioactive material quantities of concern. An example is a key implanted with an electronic chip that is only recognizable to the computer programmed in the vehicle. Only this key, and not a duplicated key, would be able to start the vehicle. Such technologies, that allow operation of a vehicle only by a means that is not easily defeated would be considered an appropriate means to disable a vehicle.

S7. The response to existing Question #72 notes that an armed response is required when there is an actual or attempted theft, sabotage or diversion of radioactive material, but the Increased Controls do not specifically require for an armed response. Therefore, is an armed response required?

An armed response is not specifically required in the Increased Controls. The IC 2. a. requirement specifies that a response to any actual or attempted theft, sabotage, or diversion of such radioactive material or of the devices simply include "requesting assistance from a Local Law Enforcement Agency (LLEA)." However, an armed response may be the preferable means to meet the objective of protecting the public health and safety. It is recognized that certain situations may necessitate an armed response, therefore a pre-arranged plan which is consistent in scope and timing with realistic potential vulnerability of sources containing radioactive material quantities of concern should be coordinated well-in-advance with LLEA in order to be prepared for various scenarios.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S8. Should I protect the identity of my license as a recipient of the Increased Controls requirements? In other words, can the indication that my license falls under Increased Control requirements be made publicly known?

It is important to protect and minimize dissemination of information that identifies recipients of the Increased Controls. The designation of a licensee as a recipient of Increased Controls is not by itself, considered sensitive. Once the full implementation of the Increased Controls has been achieved, reduced risk to materials for malevolent use is assumed. In spite of this, the identification of a licensee as an Increased Controls recipient should be minimized because the recipient can be viewed as having possession of radioactive materials that are deemed to be attractive targets for malevolent use. Licensees should use their best judgment regarding what information should be divulged, but disclosing information regarding receipt of the Increased Controls is permissible.

There are certain instances where disclosing information regarding receipt of the Increased Controls is permissible. There are circumstances where by existing regulation, licensees are required to post their licenses in an area accessible by all radiation workers. Because some licenses indicate that the licensee is required to implement the Increased Control requirements this information would be disclosed to all workers and others that are in the area of the posting. According to 10 CFR 19.11 or the Agreement State equivalent regulation, if posting of a document (i.e., a license) is not practicable, the licensee may post a notice which describes the document and states where it may be examined. However, the licensee should meet the requirements of existing statutes and regulations that require adequate posting of relevant documents for viewing. As in the case of this scenario, the licensee should use its best judgment as to the location where the license should be posted.

S9. Should information describing policies and procedures specifically for trustworthiness and reliability determinations by the licensee in response to the Increased Controls for physical protection be treated as sensitive information?

Yes. As Q&A #132 indicates, sensitive information generated by the licensee, about its physical protection of the radioactive material (including policies, plans and procedures for these Increased Controls), must be limited to individuals who have a "need-to-know" such information to perform their duties and who are considered trustworthy and reliable.

For clarification, implementing policies and procedures that detail the evaluation of trustworthiness and reliability of appropriate individuals are sensitive information if they describe the criteria for approving individuals that have the responsibility for the physical protection of information regarding the licensee's radioactive material and individuals that have unescorted access to the licensee's radioactive material.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S10. What constitutes an appropriate "tracking system" as specified in IC 3.a.1.A., which requires a licensee to use a carrier that utilizes a package tracking system during shipment?

IC 3.a.1.A. requires that licensees use carriers which use package tracking systems for shipments containing radioactive material that equals or exceeds a Table 1 value, per consignment. Such a tracking system, for the purposes of meeting the increased control requirement, must provide information concerning the accountability of, and chain of custody for the package to assist the carrier and/or licensee in determining if the shipment is lost or missing and with any subsequent investigation (e.g., last known location and intended next location, time of last communication with driver, etc.). It should be emphasized that the package tracking system used by carriers for the shipment of materials is a separate, additional requirement from the reporting requirements to be imposed under the National Source Tracking System (NSTS).

S11. Can a non-employee (i.e., consultant, contractor, etc.), who an Increased Controls recipient hires and determines is trustworthy and reliable, have access to sensitive information?

Yes. The IC 6.a. requirement states that a licensee shall control access to its physical protection information "to those persons" (not just employees) who have a need to know and are considered trustworthy and reliable. If the Increased Control recipient determines that a non-employee has the need to know based on the nature of work the individual has been hired for, and the licensee has determined that individual to be trustworthy and reliable using criteria consistent with those requirements of IC 1., then that non-employee may be granted access to sensitive information. Also, according to IC 6., the non-employee, like any other individual in receipt of or possession of sensitive information, must be aware that he/she must protect any sensitive information (such as any detailed information generated by the licensee that describes the physical protection of radioactive material quantities of concern) while in his/her possession from unauthorized disclosure.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

Version 9/20/06

S12. In order to meet the Increased Controls, is a licensee required to develop additional specific planning (contingency plans) for situations where a facility or site needs to evacuate staff due to an emergency, natural disaster, or other events where public health and safety are threatened?

The Increased Controls (ICs) do not require a licensee to develop any contingency plans; however, such planning should be done and be consistent with the intent of the ICs and the security culture being promoted. Licensees are required under 10 CFR Part 20 (and/or license condition) to ensure the security and accountability of sources. Licensees should develop contingency plans for ensuring the security and accountability of sources in the event of an evacuation or other emergency situation. These plans should, at a minimum, take into account particular events which have an increased probability of occurring in the area where the facility/site is located. Licensees should coordinate with their local law enforcement and emergency responders for developing contingency plans and must ensure that the appropriate regulatory authority is informed if the security and accountability of a source has been compromised. In the event it is determined a source should be moved away from its normal secure storage location, the licensee should notify the appropriate regulatory authority, as soon as possible, providing details on the disposition of the source(s) and the security being provided.

S13. Can a contracted carrier be inspected and held accountable by an Agreement State or the NRC for claiming to meet the Increased Controls (IC) requirements (IC 3.a.1.A.-D.) for the shipment of materials?

The NRC does not have authority under existing regulations to inspect common carriers, contract carriers, freight forwarders, warehousemen, and the U.S. Postal Service for compliance with1C 3.a.1.A.-D. Although the NRC has legal authority under Section 161.b of the Atomic Energy Act (AEA) to impose requirements on carriers, the NRC has chosen as a matter of policy to leave regulation of carriers to the Department of Transportation to avoid the possibility of dual regulation. Thus, 10 C.F.R. § 30.13, exempts common carriers, contract carriers, freight forwarders, warehousemen, and the U.S. Postal Service from the regulations of parts 30, 36, 39, and the requirements for a license in Section 81 of the AEA. In effect, § 30.13 exempts common carriers, contract carriers, freight forwarders, warehousemen, and the U.S. Postal Service from the licensing, inspection, and deliberate misconduct regulations contained in parts 30, 36, and 39. The Commission's order to "All Licensees Authorized to Possess Radioactive Material Quantities of Concern" (70 Fed. Reg. 72128 (Dec. 1, 2005)) (IC Order), imposes additional requirements on licensees. The Order does not purport to impose requirements on unlicensed and/or exempt individuals and entities. Therefore, under existing regulations, the NRC cannot inspect carriers for compliance with IC requirements. However, in some Agreement States, it is understood that some contracted or common carriers may hold general or specific licenses from the State licensing authorities. In such circumstances, the State may have inspection rights consistent with the State's regulations, the terms of the license and any orders issued to the licensee by the State.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

The above response addresses the legal ability to insist on access for purposes of conducting an inspection. NRC and Agreement State inspectors are not prevented from approaching common carriers to ask for information or access to determine compliance by licensees with Federal or State requirements. Common carriers (who are not NRC or Agreement State licensees, or have not been issued an Order) are not compelled to grant access for site visits; however, contract carriers may choose to voluntarily respond to such requests.

S14. To what extent is a licensee required to secure a room or area from unauthorized access where material is being stored behind locked doors and entry alarms? Is there a need to provide security monitoring beyond those installed on windows, doors, and access ways?

A licensee shall have a documented program to monitor and immediately detect, assess, and respond to unauthorized access to radioactive material quantities of concern and devices even if the material is being store behind locked doors and entry alarms. The key to a successful protection system is the integration of people, procedures, and equipment into a system that protects assets from malevolent adversaries. Therefore, licensees must take into account, and protect against situations where existing alarms, locks, walls, or other barriers could be defeated. Licensees can protect against the unauthorized access to and removal of material beyond typical door locks, and entry alarms through such means as guards, perimeter alarms, motion detectors, etc. The specific system and means to protect materials is by preference of the licensee; however, reasonably foreseeable means to gain access must be considered in order to meet the IC requirements. The net result of the licensee's actions to fulfill this requirement must ensure that the licensee is able to immediately detect, assess and respond to unauthorized activities.

S15. Can two or more barriers with separate locks that share the same key or lock combination qualify as "two independent physical controls" as stipulated in the IC requirement for portable and mobile devices? Also, would this apply to fixed gauges, where they would not be considered collocated if the devices do not breach the same physical barrier, but the barriers chosen share the same key or lock combination?

Yes. Two or more barriers with separate locks that share the same key or lock combination could qualify as "two independent physical controls." Whether separate locks use the same or different keys or combinations is an aspect of the licensee's access control program, and does not determine whether two barriers can be considered as "two independent physical controls." Regardless of the number of keys or combinations used, the important aspect to ensuring that there are two independent physical controls is if there exist two barriers separate and distinct from each other. The same guidance applies when considering barriers for purposes of determining if material is collocated.

As indicated in existing Q&A #59, an important aspect of a licensee's physical protection program is how the licensee will control access at the licensee's facility (see Q&A #59). If a

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

key-based system is being used, it is important that the licensee only distributes the keys to personnel that have a need-to-know and have been granted unescorted access. It is important to ensure that those who are part of a licensee's physical protection program (i.e., are in control of combinations or keys that secure material) understand the importance of their roles and responsibilities.